KNOWLEDGECUDDLE PUBLICATION

International Journal of Computer Engineering and Science, August- 2014

Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms

VekariyaMeghna
M.E.(C.E.), student
B.V.M.Engineering College
V V Nagar

***Abstract* –Today is the era of Internet and networks applications. So,Information security is a challenging issue in today's technological world. There is a demand for a stronger encryption which is very hard to crack. The role of Cryptography is most important in the field of network security. There is a broad range of cryptographic algorithms that are used for securing networks and presently continuous researches on the new cryptographic algorithms are going on for evolving more advanced techniques for secures communication. In this study is made for the cryptography algorithms, particularly algorithms- AES, DES, RSA, Blowfishare compared and performance is evaluated. Also some enhanced algorithms are described and compared with the enhanced algorithms.**

Keywords - AES, DES, BLOWFISH, Decryption, Encryption, Security

---

I. INTRODUCTION

Cryptography is a word with Greek origins, means"secret writing". However it is the science andart totransform the messages to make the secure andimmune against security attacks. It is the technique toprovide secure communication in presence of adversaries to maintain information securities such asdata confidentiality, data integrity, authentication,and non-repudiation. The process to convert ordinaryinformation or the plain text into unintelligible text orthe cipher text in cryptography is called encryption.The cipher text is understandable only to someonewho knows how to decrypt it. The message orinformation is encrypted using an encryptionalgorithm. This is usually done with the use ofan encryption key, which specifies how the messageis to be encoded. Any adversary that can see thecipher text should not be able to determine anythingabout the original message. An authorized party,however, is able to decode the cipher text usinga decryption algorithm which usually requiresa secret decryption key.There are number of cryptographic algorithms used for encryption data and most of all fall into two generic categories – Public key system and secret key system. Symmetric key algorithm is known as secrecy key or shared key algorithm. Because in symmetric key algorithm a shared key does both the encryption and decryption only one key is used for doing everything.So the success of algorithm depends on two factors-secrecy of the key and its distribution. Symmetric algorithms are: Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption algorithm (IDEA), Blowfish, AdvancedEncryption Standard (AES). Asymmetric key algorithm is also known as public key algorithm. In this algorithm, there are two keys public and private used for encryption and decryption. Public key is used to encrypt the message and private key is used to decrypt the message. Asymmetric algorithms are: Diffie-Hellman and RSA Public Key Encryption.

II. SYMMETRIC KEY ALGORITHMS

Symmetric key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

A. DES:

DES is a block cipher. It encrypts data in blocks of size 64 bits each. 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The key length is 64 bits [3]. Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness. DES results in a

permutation among the 2^64 possible arrangement of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block L and right half R. The DES algorithm turns 64-bit messages block M into a 64-bit cipher block C. If each 64-bit block is encrypted individually, then the mode of encryption is called Electronic Code Book (ECB) mode. There are two other modes of DES encryption, namely Chain Block Coding (CBC) and Cipher Feedback (CFB), which make each cipher block dependent on all the previous messages blocks through an initial XOR operation.

B. Triple DES:

Triple DES is an alternative to DES. 3DES takes a 64-bit block of data and performs the operations encrypt, decrypt and encrypt. The key is always presented as a 64-bit block, every 8th bit of which is ignored. Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows: [2] Encrypt with K1-> Decrypt with K2 -> Encrypt with K3 Decryption is the reverse process: Encrypt with K3-> Decrypt with K2 -> Encrypt with K1.

C. AES:

AES is based on a design principle known as a substitution-permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits [2]. AES operates on a 4×4 column-major order matrix of bytes, termed the state. Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128 bit keys.
- 12 cycles of repetition for 192 bit keys.
- 14 cycles of repetition for 256 bit keys.

Each round of encryption process requires the following four types of operations: Sub-Bytes, ShiftRows, MixColumns, XorRoundkey. Decryption is the reverse process of encryption and using *inverse* functions: Inv. SubBytes, Inv. ShiftRows, Inv. MixColumns.

D. RC4

RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. It takes in keys of random lengths and this is known as a producer of pseudo arbitrary numbers.The output is then XORed together with the stream of data in order to generate a newly-encrypted data.

D. BLOWFISH:

Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data- encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes [8]. The data encryption occurs via a 16-round Feistelnetwork. It is only suitable for application where the key does not change often, like communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

III. ASYMMETRIC KEY ALGORITHMS

Symmetric key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

A. RSA

RSA is a most popular and proven asymmetric cryptography algorithm. RSA is based on the mathematical fact that is easy to find the private and public keys based on the very large prime numbers. [2] **Encryption:** compute $c = m^e \bmod n$, where the e and n are the public key, and m is the message block. The c is the encrypted message. **Decryption:**

The private key *d* is used to decrypt messages. Compute: *m = c^d mod n,* where *n* is the modulus and *d* is the private key. In RSA, compare to encryption process, decryption process takes more time.

IV. ENHANCED CRYPTOGRAPHIC ALGORITHMS

A. A New Approach towards Encryption Schemes:Byte – Rotation Encryption Algorithm

It is necessary to apply effective encryption / decryption methods to enhance data security.The multiple encryption and multilevel encryption system provides sufficient security. But the performance and speed of these systems is low. Their complexity is very high. In this research paper, a new encryption algorithm named"**Byte – Rotation Encryption Algorithm (BREA)"** is proposed which is applied on different blocks of plaintextand executes in parallel manner through multithreading concept of single processor system. This paper is an attempt to invent a new encryption model which is more secure and very fast to others.
The BREA algorithm has the following features…

1. It is a Symmetric Key Block Cipher Algorithm.
2. Each block size is of 16 bytes.
3. Size of Key matrix is 16 bytes.
4. Values of Key matrix are randomly selected and ranging from 1 to 26.
5. Mono alphabetic substitution concept is followed.
6. Byte-Rotation technique is used.

The steps of proposed Byte-Rotation Encryption Algorithm:

1. The letters of alphabet are assigned numerical valuesfrom 1 to 26 in sequence i.e. A, B, C, ..., X, Y, Zassigned numerical values 1, 2, 3, ..., 24, 25, 26respectively, the digits from 1 to 9 assigned numericalvalues from 27 to 35 respectively and the zero (0)remains as it is.
2. The plaintext is partitioned into fixed-length blocks ofsize 16 bytes (or 128 bits) each. These blocks arerepresented by a matrix Mp.
3. The values of Key matrix (K) are randomly selectedfrom the range 1 to 26. The size of Key matrix isequivalent to the block size of plaintext i.e. 16 bytes.

K = [k1, k2, ..., k16]
K = Random (1, 26, 16)

4. Calculate the Transpose matrix of plaintext blockmatrix (Mp), which is denoted by MpT.
5. Calculate encrypted Key matrix Ke using the followingformula:Ke = K mod 2
6. Add both the matrices MpT and Ke and the resultantmatrix is denoted by Cpk.Cpk = MpT + Ke
7. Rotate first three rows horizontally of Cpk matrix suchthat rotate one byte from first row, rotate two bytesfrom second row, rotate three bytes from third rowand fourth row remains untouched. The resultantmatrix is denoted by Chr .
8. Rotate first three columns vertically of Chr matrix suchthat rotate one byte from first column, rotate two bytes from second column, rotate threebytes from thirdcolumn and fourth column remains untouched. Theresultant matrix is denoted by Cvr.
9. Replace numeric values of Cvr matrix by theircorresponding letters and if 36 exist in Cvrmatrix, it isreplaced by the special character #. The resultantmatrix is denoted by Ce.

Block Wise Parallel Encryption System which is differentand efficient from the existing systems as follows:

1. System is developed in such a way that it is platformindependent. Where, the existing systems are limited toplatform dependent design.
2. It is developed with the idea of multiple and multilevelencryption system.
3. The number of encryption algorithms is used; hence thesecurity offered is very high.
4. This proposed system is developed in order to support notonly text files but also images and media files. But stillmany of the existing systems are developed in order to suitbasic text formats.
The input plaintext which is to be fed into our system ischosen at first. Then, a key phrase is entered for dataauthentication. Then plaintext data is divided into blocks.
Four blocks passed into four threads of BREA at a time.These threads executes simultaneously by usingmultithreading technique. After encryption, these blockssend to receiver where the blocks are passed into theReverse – BREA in parallel manner. Then the cipher text I decrypted into plaintext and all the blocks of plaintextscrambled together to get

the original message. Since thealgorithm executes parallel using multithreading technique,the execution speed and performance of the model increases.

Multithreading:

It is an ability of OS to support multiplethreads of execution within a single process. A thread is asmall block of a program / execution unit.

Uses of Multi-Threading:

- Division of work
- Foreground & background work
- Asynchronous processing
- Pipeline/Parallel execution
- Organization of work
- Modular program structure

Benefits of Threads:

- Takes less time to create a new thread than aprocess
- Less time to terminate a thread than a process
- Less time to switch between two threads within thesame process
- Threads within the same process share memory andother resources, they can communicate with eachother without invoking the kernel. So the modelis very fast to other suggested models.

B. Advanced Encryption Algorithm Using Fuzzy Logic

Today the security is the main issue in data communication. Encryption can provide a fine solution for it. The encryption algorithm is the mathematical procedure for performing encryption on data. After conducting a research on currently using encryption algorithms, we have identified that all these algorithms only concern about security. But consuming a less processing power is also equally important as the security for connections with low bandwidths. The proposed algorithm supports for user desired security level and processing level. It is a block cipher which is a derivation on the feistelnetwork architecture. The algorithm provides security levels and their corresponding processing levels by using various keys for the encryption/decryption process. This facility is achieved by using fuzzy logic. The results of the proposed encryption algorithm will be analyzed by comparing with other existing encryption algorithms. Finally the aim of the research is to come up with an encryption algorithm which can provide either low processing or high security according to user's requirement which will be more advanced than the existing encryption algorithms.

Implementing fuzzy logic:

Fuzzy logic is a problem-solving control system methodology that presents itself to implementation in systems ranging from simple, small, embedded micro-controllers to large, networked, multi-channel PC or workstation-based data acquisition and control systems. Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing input information. Infuzzy logic rules and membership sets are used to make a decision. To achieve security and low processing, the algorithm uses variable keys. 0th position gives a fully low processing algorithm and 1stposition gives fully secured algorithm. The fuzzification changes depending on the key size and the number of mapping tables of the encryption algorithm. Users can input the desired key. One character will be 8 bit long. The main algorithm structure defines different key sizes up to 128bit. User can enter desired key-(application defines as the password) and also depending on the number of mapping tables' algorithm would allocate weight dynamically. Allocation of the weights will differ from 0.0 to 1.0 range; and the number of security levels would be vary from 1-16.The number of rounds will be determined by pre-defined mapping tables and the users initial input. Mapping tables are predefined in the algorithm and consists of mathematically defined values, and then those values will dynamically choose the relevant algorithm procedure once the user input the key to encryption.

Best case Scenario-Sample user input the key size of 16 Byte value and provides mapping table number which can be differentiated between 1 and 8. Assume that the user has selected the option of encrypting with the number 8 mapped table. The algorithm will allocate a higher weight to the provided user inputs since the initial key size is 16 Bytes that will resulted in providing the highest number of rounds which is 16. Eventually the highest value of input key size will derive a higher weight thus making the highest level of rounds and the highest level of security.

Worst case Scenario-Sample user input the key size of 1 Byte value and provides mapping table numberwhich can be differentiated between 1 and 8. Assume that the user has selected the option of encrypting with the number 1 mapped table. The algorithm will allocate a lower weight to the provided user inputs since the initial key size is 1 Bytes,

eventually the lowest value of input key size will derive a lower weight. Then it will be reflected in the security rounds of the algorithm and which will be resulted in lowest level of security.

Normal day Scenario-Sample user input the key size of 8 Byte value and provides mapping table number which can be differentiated between 1 and 8. Assume that the user has selected the option of encrypting with the number 4 mapped table. The algorithm will allocate a higher weight than the worst case scenario but lower weight that the best case scenario to the provided user inputs since the initial key size is 8 Bytes, eventually the modest value of input key size will derive a middle weight value. Then it will be derived the number of security rounds which in this case is 8 and then the modest level of security will be enforced in the algorithm. Following are some of fuzzy logic rules.

• If Key length is 1 byte and the Level is 0 : number of Cycles is 0
• If Key length is 2 byte and the Level is 0 : number of Cycles is 1
• If Key length is 3 byte and the Level is 0 : number of Cycles is 1
• If Key length is 4 byte and the Level is 0 : number of Cycles is 2

Like this there are 144 fuzzy rules.

C. Advance cryptography algorithm for improving data security

The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the algorithm improves encryption security by inserting the symmetric layer. The algorithm will be useful to the applications which require the same procedure of encryption and decryption.

Proposed Key Generation Steps:

1. Select or create any private key of Size 256 X 2 bits or 64 characters.
2. Size of selected key will be varying from 128 bits to 512 bits or 16 to 64 characters.
3. We can choose any character from 0 to 255 ASCII code.
4. Use of 64 * 8 key that means 512 bits in length.
5. Divide 64 bytes into 4 blocks of 16 bytes likes Key_Block1, Key_Block2, Key_Block3, and Key_Block4.
6. Apply XOR operation between Block1 and Block3. Results will store in new Key_Block13.
7. Apply XOR operation between Block2 and Block13. Results will store in new Key_Block213.
8. Apply XOR operation between Key_Block213 and Key_Block4. Results will store in new Key_Block4213.
9. Repeat Step 7, 8, 9 till (random number / 4).
10. Exit

Steps of proposed Algorithm:

1. Initially select plane text of 16 bytes (or we can vary from 16 to 64 depend on requirement).
2. Initially insert key of size 16 bytes (depend on plane text value)
3. Apply XOR operation between key (Key_Block4213) and plain text block (Text_Block). Result will store in Cipher Block1.
4. Apply right circular shift with 3 values. Result will store in new Cipher_Block2.
5. Apply XOR operation between Cipher_Block2 and Key_Block2. Result will store in new Cipher_Block3.
6. Apply XOR operation between Cipher_Block3 and Key_Block4. Result will store in Cipher_Block4.
7. Cipher_Block4 is the input of the next round as a plane text block.
8. Repeat step 1 to 7 till (Encryption Number / 4).
9. Exit.

The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value.

V. EXPERIMENTAL RESULTS

AES and Blowfish algorithms can be implemented to different audio files. Comparison of encryption time has been given in the following table 1, and it shows the Average time of AES and BLOWFISH algorithm for different audio files encryption. Next, Comparison of decryption time has been given in the following table 2, and it shows the Average time of AES and BLOWFISH algorithm for different audio files decryption. Table 3, shows comparison of various cryptographic algorithms based on different factors.

Table 1: Average time of Encryption

Audio Files (KB)	Encryption time of BLOWFISH (MS)	Encryption time of AES (MS)
8,282	970	1025
387	38	55
33	16	20
2,826	348	370
Average Time	343	367.5

Table 2: Average time of decryption

Audio Files (KB)	Encryption time of BLOWFISH (MS)	Encryption time of AES (MS)
8,282	300	433
387	120	220
33	21	28
2,826	55	97
Average Time	124	194.5

Table 3: Comparison of different cryptographic algorithms

Algorithm	Key Size(s)	Speed	Speed Depends On Key?	Security
DES	56 bits	Slow	Yes	Insecure
3DES	112/168 bits	Very Slow	No	Moderately secure
AES	128, 192, 256 bits	Fast	Yes	Secure
BLOW-FISH	32-448 bits	Fast	No	Believed secured, but less attempted crypt-analysis than other algorithms
RC4	256 bytes	Very Fast	No	Moderately secure
RSA	1024 bits and above	Fast	Yes	Secure

Here, **The Advanced cryptographic Algorithm** (with 265bit block size in this thesis) and "**A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"** algorithm (with 128-bit block size) and **"Effect of Security Increment to Symmetric Data Encryption through AES Methodology"** algorithm (with 128-bit block size) have been implemented on a number of different data files like text, pdf and image varying types of content and sizes of a wide range. But here we are only showing result of text file. Encryption and Decryption time of Various Text files comparisons shown in table 4 and table 5 respectively.

Table 4: Encryption time comparison of text files

Plain Text Size	DJSA algorithm	Data Encryption through AES Methodology	Proposed Algorithm
1.66 mb	0:01:34	0:01:32	0:01:25
560 kb.txt	0:00:37	0:00:35	0:00:28
187 kb.txt	0:00:18	0:00:16	0:00:09
46 kb.txt	0:00:11	0:00:09	0:00:02
16 kb.txt	0:00:10	0:00:08	0:00:01

Table 5: Decryption time comparison of text files

Plain Text in Size	DJSA symmetric key algorithm	Data Encryption through AES Methodology	Proposed Algorithm
1.66 mb.txt	0:01:34	0:01:32	0:01:25
560 kb.txt	0:00:37	0:00:35	0:00:28
187 kb.txt	0:00:18	0:00:16	0:00:09
46 kb.txt	0:00:11	0:00:09	0:00:02
16 kb.txt	0:00:10	0:00:08	0:00:01

VI. CONCLUSION

Cryptography algorithm is the science in secret code. Rapidly rising cybercrime and the growing prospect of the internet being used as a medium for attacks create a major challenge for network security. Some well-known cryptographicalgorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques.It was concluded that Blowfish has better performance than AES in terms of Average time.“**Byte – Rotation Encryption Algorithm (BREA)”** allows all the blocks to processparallel in CPU. Because of parallel execution, theprocessing speed of the system will enhance. Encryption algorithm using fuzzy logic which can provideeither low processing or high security according to user’s requirement which will be more advanced than theexisting encryption algorithms. From the result it is clear that our “Advanced technique” is batter result producing as compared “DJSA symmetric key algorithm” and “Effect of Security Increment to Symmetric Data Encryption through AES Methodology”. If any user emphasis on security then he can use our proposed algorithm. No one can guarantee 100% security. But we can work toward 100% risk acceptance. A good cryptographic system strikes a balance between what is possible and what is acceptable. Thus considerable research effort is still required for secured communication.

REFERENCES

[1] AtulKahate “cryptography and network security”, Tata McGraw-Hill publishing company, New Delhi, 2008.
[2] William Stallings, “Network Security Essentials(Applications and Standards)”, Pearson Education,2004.
[3] W. Stallings, “Cryptography and Network Security”, Prentice Hall, 1995.
[4] National Bureau of Standards, “Data EncryptionStandard, ” FIPS Publication 46, 1977.
[5] DriptoChatterjee, JoyshreeNath, SuvadeepDasgupta, AsokeNath “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.
[6] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994
[7] SairamNatarajan #1,“A Novel Approachfor Data Security Enhancement Using MultiLevel Encryption scheme”, Researchpaper, IJCSIT, Vol. 2 (1), 2011, 469-473.
[8] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.
[9] Neal Koblitz “A Course in Number Theory and Cryptography” Second Edition Published by Springer-Verlag.
[10] By Klaus Felten “An Algorithm for Symmetric Cryptography with a wide range of scalability” published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT.